

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 614 159 A1

(12)

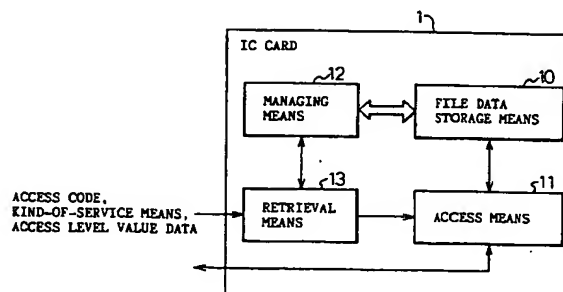
EUROPEAN PATENT APPLICATION
published in accordance with Art.
158(3) EPC

(21) Application number: **93924173.3**(51) Int. Cl.⁵: **G06K 19/00, G06K 17/00**(22) Date of filing: **04.11.93**(86) International application number:
PCT/JP93/01595(87) International publication number:
WO 94/10655 (11.05.94 94/11)(30) Priority: **04.11.92 JP 294863/92**(43) Date of publication of application:
07.09.94 Bulletin 94/36(84) Designated Contracting States:
FR(71) Applicant: **FUJITSU LIMITED**
1015, Kamikodanaka
Nakahara-ku
Kawasaki-shi Kanagawa 211 (JP)(72) Inventor: **MIYAZAKI, Junsuke**
Fujitsu Limited,**1015, Kamikodanaka,**
Nakahara-ku**Kawasaki-shi, Kanagawa 211 (JP)**Inventor: **HARA, Hideaki, Fuji Research**
Institute Corporation
2-12, Kaigan 3-chome,
Minato-ku
Tokyo 108 (JP)(74) Representative: **Joly, Jean-Jacques et al**
Cabinet Beau de Loménie
158, rue de l'Université
F-75340 Paris Cédex 07 (FR)(54) **IC CARD.**

(57) Security protection is accomplished in an IC card by achieving security protection of data at an item level, allowing a high speed access, and preventing illegal use. The IC card includes means (12) for managing service-wise an access level value allotted to each data item, means (13) for retrieving a data item designated by access level value information from outside by looking up a management access level value designated by service kind information from outside, and means (11) for gaining access collectively to the data item values retrieved. The IC card further includes means (23) for initiating time count processing from an initial value whenever a normal access processing is completed, means (24) for judging whether or not data is greater than a time limit value of time count graphic definition, and means (25) for reporting an error occurrence to outside when a time-over state of the time count

value is judged.

Fig.4



TECHNICAL FIELD

The present invention relates to an IC card and, particularly, to an improved novel IC card which enables not only high-speed access but also realizing the data security at an item level as well as to an IC card which realizes the data security by preventing unauthorized access.

BACKGROUND ART

Use of IC cards becomes popular as the information technologies are developed. Since important personal data are stored in the IC cards, it is necessary to provide IC cards the functions which do not permit unauthorized access to the data of individual persons.

Fig. 1 shows a method of making access to an IC card that has heretofore been proposed. Referring to the IC card 1 of Fig. 1, PIN which is a personal identification number of a card owner, a key which is a password formed by the terminal equipment, a file name at the destination of access, and access right are input to the IC card in compliance with a program in the terminal equipment in which the IC card is inserted. Access is permitted to a designated file data when the PIN that is input is in agreement with a PIN key that has been set in a file at a destination of access, when a key that is input is in agreement with a key that has been set in the file at the destination of access, and when access right that is input is in agreement with access right that has been set in the file at the destination of access. The file data to which access is permitted comprises a plurality of data items as shown in Fig. 2.

Here, the access right stands for such kinds of right as right for reading the IC card, right for writing on the IC card and right for reading and writing on the IC card. The "Item No." in Fig. 2 may not often be stored as data in the file data and, when addresses have been determined for each of the data, the "Name of Data Item" in Fig. 2 may not often be stored as data.

According to such an access method, protection of secrecy of data is realized with the file data as a unit arousing a problem in that access can be obtained to data items which have not really been aimed at by the program. That is, referring to the example of Fig. 2, it becomes possible to make access to the data item "OFFICE" in a file even though the program is not really making access to this data item. Thus, the secrecy of data is not protected.

To cope with this problem, the present applicant has previously filed a patent application entitled "SYSTEM FOR PERMITTING ACCESS TO DATA FIELD AREA IN IC CARD FOR MULTIPLE

SERVICES" (see Japanese Unexamined Patent Publication (Kokai) No. 63-73348).

In the file data according to this system as shown in Fig. 3, the access code (AC code)/access right are set for each of the data items. Therefore, access to the data item is permitted only when the access code/access right input through the terminal equipment are in agreement with the access code/access right that have been set to a data item for which access is requested. Here, PIN may be set for each of the data items in addition to the access code and access right.

According to this example, whether access be permitted or not is controlled with each data item as a unit making it possible to reliably protect the secrecy of data of the IC card. To make access to a plurality of data items, however, the access processing must be executed a plurality of times causing a new problem in that the speed of access to the data becomes slow.

According to the conventional IC card described above, on the other hand, no active processing is carried out on the side of the IC card after the IC card is inserted in the terminal equipment even though no access request is output from the program of the terminal equipment for a long period of time. That is, the processing is carried out only according to the program of the terminal equipment.

When no active processing is executed on the side of the IC card, however, there remains a problem in that the IC card may be used by an unauthorized person who is not the owner of the card. For instance, an authorized card owner who is just changing the PIN may happen to leave the terminal equipment for some reason. Then, another unauthorized person may set a new PIN to the IC card and may leave the place carrying it with him. Should that happen, personal data of the authorized card owner may be used without authorization and the secrecy can no longer be maintained.

Moreover, in case trouble occurs on the side of the terminal equipment while access is being made to the IC card and access is incompletely finished, updating of the data in the IC card may end unfinished. In fact, however, attention has not been much given to restoring the data in the IC card by the IC card itself, and laborious work is required for restoring the data.

DISCLOSURE OF THE INVENTION

The present invention was accomplished in view of the above-mentioned circumstances, and its object is to provide a novel IC card which realizes the protection of secrecy of data at an item level and, at the same time, permits access to be made at a high speed.

Another object of the present invention is to provide a novel IC card which realizes the protection of secrecy of data by preventing the unauthorized use.

A further object of the present invention is to provide a novel IC card capable of restoring the data from the updating of incomplete data caused by trouble on the side of the terminal equipment.

In order to achieve the above-mentioned objects, the present invention provides an IC card for managing item values of a plurality of data items utilized for one or a plurality of services, comprising:

managing means for managing, depending upon the services, access level values and access rights allocated for the data items;

retrieval means which, when a kind-of-service data and an access level value data are given as an access code from an external unit, makes reference to the management data of said managing means designated by said kind-of-service data, and retrieves a data item designated by said access level value data on condition of having an access right; and

access means which batchwisely makes access to the item values of the data items retrieved by said retrieval means.

In order to achieve the above-mentioned objects, furthermore, the present invention provides an IC card for executing access to file data that are to be managed in response to a request of access from an external unit, comprising:

timer means which begins a counting processing starting with an initial value every time when a normal access processing is finished;

judging means for judging whether a value counted by said timer means is larger than a time-limit value or not; and

notifying means which notifies the occurrence of error to the external unit when the counted value is judged by said judging means to be out of time.

In order to achieve the above-mentioned objects according to the present invention, furthermore, provision is made of a recording means for recording access history and restoring means for restoring the data into the state at the time of beginning the processing, in addition to the above-mentioned timer means and the judging means.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 is a diagram for explaining a first conventional IC card;

Fig. 2 is a diagram illustrating a first example of file data stored in the IC card of Fig. 1;

Fig. 3 is a diagram illustrating a second example of file data stored in the IC card of Fig. 1;

Fig. 4 is a diagram illustrating the constitution of an IC card according to a first embodiment of the present invention;

Fig. 5 is a diagram illustrating a first example of contents stored in the managing means and in the file data storage means of Fig. 4;

Fig. 6 is a flow chart explaining the process flow of an IC card equipped with managing means and file data storage means of Fig. 5;

Fig. 7 is a diagram explaining the outputs of results of access by the process flow of Fig. 6;

Fig. 8 is a diagram illustrating a second example of the contents stored in managing means and in file data storage means of Fig. 4;

Fig. 9 is a flow chart explaining the process flow of an IC card equipped with managing means and file data storage means of Fig. 8;

Fig. 10 is a diagram explaining the outputs of results of access by the process flow of Fig. 9;

Fig. 11 is a diagram illustrating the constitution of an IC card according to a second embodiment of the present invention;

Fig. 12 is a first time chart for explaining the operation of the IC card of Fig. 11;

Fig. 13 is a second time chart for explaining the operation of the IC card of Fig. 11; and

Fig. 14 is a third time chart for explaining the operation of the IC card of Fig. 11.

BEST MODE FOR CARRYING OUT THE INVENTION

A first embodiment of the present invention will now be described in detail in conjunction with the drawings.

Fig. 4 illustrates the constitution of an IC card realizing the protection of secrecy of data yet enabling high-speed access to be carried out. The IC card shown in Fig. 4 manages values of a plurality of data items used for one or a plurality of services, and has a file data storage means 10, an access means 11, a managing means 12, and a retrieval means 13.

The file data storage means 13 stores the values of the plurality of data items pertaining to the files with a file as a unit. The access means 11 makes an access to the values of data items stored in the file data storage means 10. The managing means 12 stores the name DI, the key KY and the personal identification number PIN for the group of data items, and further stores, for each of the services, the access level value and the access right allocated for each of the data items. The retrieval means 13 retrieves the data managed by the managing means 12 and determines the data item at a destination of access.

According to another example, the managing means 12 manages a specific access level value

specific to a data item that is used in common for all services, and manages, depending upon the services, the specific access level value to which link will be made and the access right allocated for each of the data items.

Fig. 5 illustrates a first example of management data stored in the managing means 12 of the IC card 1 and of the values of data items stored in the file data storage means 10. Fig. 5 shows the management data stored in the managing means 12 together with the values of data items stored in the file data storage means. That is, the values of data items shown on the extreme right side are stored in the file data storage means 10, and the data on the left side thereof are stored in the managing means 12 as management data.

The managing means 12 stores the group of data items (DI), key (KY) and personal identification number (PIN) for all of the management data, and stores, depending upon the services, the access level values and access rights allocated to the data items. As for the name of data item "NAME", for instance, the managing means 12 stores an access level value "0"/write right "R" allocated to the service A, access level value "01"/write right "R" allocated to the service B, and access level value "01"/write right "R" allocated to the service C.

As for the name of data item HOME ADDRESS, the managing means 12 stores the access level value "02"/read-write right "RW" allocated to the service A, access level value "03"/read-write right "RW" allocated to the service B, and access level value "02"/read right "R" allocated to the service C.

Here, by taking an example of bank service, the access level value stands for the height of level for permitting access such as access level value "10" for the manager of a branch office, access level value "05" for a general bank employee, and access level value "99", for a card owner.

In the example shown in Fig. 5, the PIN is used in common for a group of data items. It is, however, allowable to set PINs for each of the data items. For instance, access level value "01"/access right "R"/PIN "00289456" may be set for the service A, and access level value "01"/access right "R"/PIN "00289434" may be set for the service B of the name of data item, "NAME".

Described below is how to process the thus constituted IC card.

First, the operation will be briefly described. The retrieval means 13 is served, from an external terminal equipment, with a designated file name, a key, a PIN, and as an access code, a kind-of-service data and an access level value data. In accordance with the management data in the managing means 12, the retrieval means 13 specifies a group of data items relying upon the designated

file name, and makes reference to the key and PIN. The retrieval means 13 then makes reference to the access level values that are classified into the designated kind-of-service data on condition of having an access right that matches with the designated access right. The retrieval means 13 then specifies a data item having an access level value smaller than the access level value data that is input.

As the retrieval means 13 thus retrieves a plurality of data items designated by the access codes, the result of retrieval is then handed over to the access means 11. By using the retrieved data items, the access means 11 makes a batchwise access to the values of data items stored in the file data storage means 10. The access means 11 outputs the result of access to an external unit.

Thus, a plurality of items can be executed through one time of access processing; i.e., high-speed access can be realized while realizing the protection of secrecy of data at the item level.

In the foregoing description, the retrieval means 13 specifies a data item having an access level value smaller than the access level value that is input. It is, however, also allowable instead to set an access level value so as to specify a data item that has a large access level value.

The process flow for executing the above-mentioned IC card will now be described by using a flow chart of Fig. 6.

At a step 1, the IC card 1 specifies a group of data items designated by the file name that is input. That is, a group of data items as shown in Fig. 5 among a plurality management data, is specified as a group of data items to which access is requested.

Then, a step 2 collates the PIN that is input with the PIN possessed by the specified group of data items. When it is judged at a step 3 that the two are not in agreement, the program ends as an error. When it is judged that the two PINs are in agreement, the program proceeds to a step 4 where the key that is input is collated with the key possessed by the specified group of data items. When it is judged at a step 5 that the two are not in agreement as a result of collation, the program ends as an error. When it is judged that the two keys are in agreement, the program proceeds to step 6 where it is checked whether the service name that is input has been registered in the specified group of data items or not.

When it is judged at a step 7 as a result of checking that the service name that is input has not been registered, the program ends as an error. When it is judged that the service name has been registered in the specified group of data items, the program proceeds to a step 8 where reference is made to access level values that are classified into

input service names included in the specified group of data items, and the name of data item having an access level value smaller than the input access level value is specified on condition of having access right that matches with the access right that is input. Finally, a step 9 makes a batch-wise access to the data item value possessed by the name of the specified data item, thereby to complete the processing.

In the above-mentioned embodiment, when an access code, i.e., access level value "02" of service B, is input from the terminal equipment, access can be made to the result of access shown in Fig. 7 through one time of access processing. As described above, the IC card of the present invention is capable of executing the processing for making access to a desired data item through one time of access processing and by designating only one access code yet realizing the protection of secrecy of data on the item level.

Described below is another example of the managing means 12.

Fig. 8 illustrates a second example of the management data stored in the managing means 12 and the data item values stored in the file data storage means 10. Here, Fig. 8 illustrates specific access level values and further illustrates only those portions that are different from the management data of Fig. 5. Nearly the same holds even in the following description of processing operation.

The managing means 12 shown in Fig. 8 stores specific access level values that are common for the group of data items and, further stores, depending upon the services, the specific access level values at destinations of links allocated to the data items. As for the specific access level values that will be used in common, there are shown destinations of links that have the same or smaller specific access level values and are closest thereto but that have not been linked yet.

As for the specific access level values allocated to the data items, for example, as for the name of data item "HOME ADDRESS", the managing means 12 stores specific access level value "10" at a destination of link allocated to the service A, specific access level value "10" at a destination of link allocated to the service B, and specific access level value "ED" at a destination of link allocated to the service C.

As for the name of data item "HOME PHONE NO.", the managing means 12 stores specific access level value "20" at a destination of link allocated to the service A, specific access level value "20" at a designation of link allocated to the service B, and specific access level value "20" at a destination of link allocated to the service C. Though not diagramed in Fig. 8, the managing means 12 further stores the kinds of access rights.

In Fig. 8, symbol "ED" denotes a final data which has the lowest specific access value in the service and has the address value to be linked of "00".

Described below is how to process the IC card that uses the above-mentioned second management data.

First, the operation will be described briefly. The retrieval means 13 is served, as an access code from an external unit, with a kind-of-service data and an access level value data. In accordance with the management data in the managing means 12, the retrieval means 13 specifies a group of data items like the one shown in Fig. 8 relying upon the file name that is designated. The retrieval means 13 then uses the access level value as an initial specific access level value on condition of having access right that matches with the designated access right. The retrieval means 13 makes reference to specific access level values that agree with the specific access level values that are commonly used for the group of data items, successively traces the specific access level values designated by the destinations of link included in the data items possessed by the service data thereby to specify the specific access level values to be linked and hence to specify the data items having the specific access level values to be linked.

The processing executed by the above-mentioned IC card will be described by using a flow chart of Fig. 9. In this flow chart, the processings from a step 1 to a step 7 are the same as those explained in the process flow of Fig. 6. That is, it is judged whether the PIN/KEY possessed by the group of data items designated by the input file name is in agreement with the PIN/KEY that are input and, besides, whether the service name input to the group of data items has been registered therein or not.

The program then proceeds to a step 8 where the processing is repetitively carried out to first specify a specific access level value of a destination of link stored being corresponded to a specific access level value that is in agreement with an input access level value, to specify a specific access level value of a destination of link stored being corresponded to the specific access level value that agrees with the above specific access level value in the destination of link, and then to specify a specific access level value in a destination of link stored being corresponded to the above specific access level value that agrees with the specific access link value in the destination of link. This makes it possible to specify the name of the data item designated by the specific access level value that is to be linked to the input access level value. The name of data item having access right that matches with the input access right is specified out of the names of the thus specified data

items.

When an access code, i.e., input access level value "30" of service A is input through the terminal equipment while managing means 12 is storing the data shown in Fig. 8 according to a particular processing of the names of data items based upon the link trace processing, then, there are specified the names of three items, i.e., "HOME PHONE NO." having a specific access level value "30", "HOME ADDRESS" having a specific access level value "20", and "NAME" having a specific access level value "10".

Then finally at a step 9, access is made batchwisely to the data item values possessed by the specified names of the data items to finish the processing. The results of this access are shown in Fig. 10.

When the managing means 12 employs the data storage structure of Fig. 5 without taking the access right into consideration, access will be made to all of the data items of lower than the input access level value. When the managing means 13 employs the data storage structure of Fig. 8, on the other hand, access will be made to the data items that are linked to the input access level value; i.e., the managing means 12 employs the data managing structure of Fig. 3, enabling the objects of access to be flexibly selected.

By executing the process flow of Fig. 9 as described above, the IC card of the present invention carries out access processing to desired data items through only one time of access processing requiring only one access code to be designated, yet realizing the protection of secrecy of data at the item level.

A second embodiment of the present invention will now be described. This embodiment intends to prevent the data from being used in an unauthorized manner in order to realize the protection of secrecy of data.

The IC card 1 shown in Fig. 11 is provided with a file data storage means 20, an access means 21, a recording means 22, a timer means 23, a judging means, 24, a notifying means 25 and a restoring means 26.

The file data storage means 20 stores the data with a file as a unit. The access means 21 makes access to the data stored in the file data storage means 20. The recording means 22 records the access history to the file data from the start of processing. The timer means 23 is reset every time when the normal access processing is finished and, then, executes the counting processing starting with the initial value. The judging means 24 judges whether the value counted by the timer means 23 is larger than a predetermined time-limit value or not. The time-limit value may represent a different value depending upon the services. The

notifying means 25 notifies the occurrence of error to the external unit and to the notifying means 26 which restores the data stored in the file data storage means 20.

According to this embodiment which is provided with the timer means 23, judging means 24 and notifying means 25, the occurrence of error is notified to an external unit in case the normal access processing is not carried out within a predetermined period of time. When a normal card owner who is changing the PIN leaves his place for some reason as mentioned earlier, error is notified when a time-limit value is exceeded. It is therefore made possible to prevent unauthorized deed such as another person may set a new PIN to the IC card. Therefore, not only the protection of secrecy of data is realized but also any trouble in the terminal equipment is notified as the occurrence of error is notified.

With the recording means 22 being provided, furthermore, the source of requesting access, in case error has occurred, is allowed to resume the processing while making sure the degree of transaction accomplished. With the recording means 22 and the restoring means 26 being provided, furthermore, the file data can be automatically restored to the state of when the processing is started in case error has occurred.

The processing executed by the IC card will now be described with reference to time charts of Figs. 12 to 14.

As shown in the time chart of Fig. 12, in executing the access processing to the file data by the IC card, the timer means 23 is driven when the access processing is normal, and error is notified to the terminal equipment when the value counted by the timer means 23 becomes greater than a predetermined time-limit value.

Here, if a constitution is employed to manage the time-limit value depending upon the services and to use a time-limit value designated by the name of service designated by an access code, then it is allowed to use a suitable time-limit value for each of the services. When the IC card is not equipped with the source of generating clocks, then the IC card executes the counting processing of the timer means 23 by using clock signals fed from an external unit.

By using the IC card of this embodiment as described above, occurrence of error is notified to the external unit in case the normal access processing is not carried out within a predetermined period of time, making it possible to prevent unauthorized use. Thus, the protection of secrecy of data is realized. In case the terminal equipment becomes defective, this fact is notified as the occurrence of error is notified.

The timer discontinues its operation when the normal processing is finished. Here, the end of the normal processing is judged either by the IC card itself or by the instruction on the side of the terminal equipment. In either case, judgement is rendered by a command from the terminal equipment, and means therefor is not specified in the present invention.

As shown in the time chart of Fig. 13 which employs this processing constitution, in case error occurs as a result of time over while recording the completion of access processing from the start of the processing, the source of requesting access is allowed to make sure the degree of transaction that is accomplished and to resume the processing. On the other hand, when it is requested at the time of occurrence of error to cancel the access processing from the start of the processing, then the access history in the access processing is recorded from the start of the processing as shown in the time chart of Fig. 14, and the file data at the time of starting the processing is restored at a moment when error has occurred as a result of time over.

The timer discontinues its operation when the normal processing is finished. Here, the end of the normal processing is judged either by the IC card itself or by the instruction on the side of the terminal equipment. In either case, judgement is rendered by a command from the terminal equipment, and means therefor is not specified in the present invention.

According to the present invention as described above, there is provided an IC card which enables high-speed access to be carried out while realizing the protection of secrecy of data at the item level. There is further provided an IC card which prevents unauthorized use to realize the protection of secrecy of data.

The invention further makes it possible to normally function the system even when the terminal equipment is not provided with a timer function or even when the timer function of the terminal equipment fails to normally operate. A further advantage of the present invention is that in case the terminal equipment or the host becomes defective, the unfinished processing is invalidated and the data in the IC card are restored.

List of Reference Numerals

- 1 IC card
- 10 file data storage means
- 11 access means
- 12 managing means
- 13 retrieval means
- 20 file data storage means
- 21 access means
- 22 recording means

- 23 timer means
- 24 judging means
- 25 notifying means
- 26 restoring means

Claims

1. An IC card for managing item values of a plurality of data items utilized for single or plurality services, comprising:
 - managing means (12) for managing, depending upon the services, access level values and access rights allocated for the data items;
 - retrieval means (13) which, when a kind-of-service data and an access level value data are given as an access code from an external unit, makes reference to the management data of said managing means (12) designated by said kind-of-service data, and retrieves a data item designated by said access level value data on condition of having an access right; and
 - access means (11) which makes access at a stretch to the item values of the data items retrieved by said retrieval means (13).
2. An IC card according to claim 1, wherein the retrieval means (13) retrieves data items of access level values smaller than an access level value given from an external unit.
3. An IC card according to claim 1, wherein the retrieval means (13) retrieves data items of access level values larger than an access level value given from an external unit.
4. An IC card according to claim 1, wherein the managing means (12) manages, depending upon the services, the specific access level values specific to the data items and the specific access level values of destinations of link allocated to said data items.
5. An IC card according to claim 4, wherein the retrieval means (13) retrieves data items of access level values smaller than an access level value given from an external unit.
6. An IC card according to claim 4, wherein the retrieval means (13) retrieves data items of access level values larger than an access level value given from an external unit.
7. An IC card for executing access to file data that are to be managed in response to a request of access from an external unit, comprising:

timer means (23) which begins a counting processing starting with an initial value every time when a normal access processing is finished;

judging means (24) for judging whether a value counted by said timer means (23) is larger than a time-limit value or not; and

notifying means (25) which notifies the occurrence of error to the external unit when the counted value is judged by said judging means (24) to be longer than a time-limit value.

8. An IC card according to claim 7, wherein provision is made of a recording means (22) for recording the access history for the file data from the start of the processing.
9. An IC card according to claim 8, wherein provision is made of a restoring means (26) for restoring the file data to the state of starting the processing in accordance with the data recorded in the recording means (22) when the notifying means (25) notifies an error to the external unit.
10. An IC card according to claim 7, wherein the timer means (23) executes the counting processing by using clock signals generated from a clock source in the IC card.
11. An IC card according to claim 7, wherein the timer means (23) executes the counting processing by using clock signals given from an external unit.

Fig.1

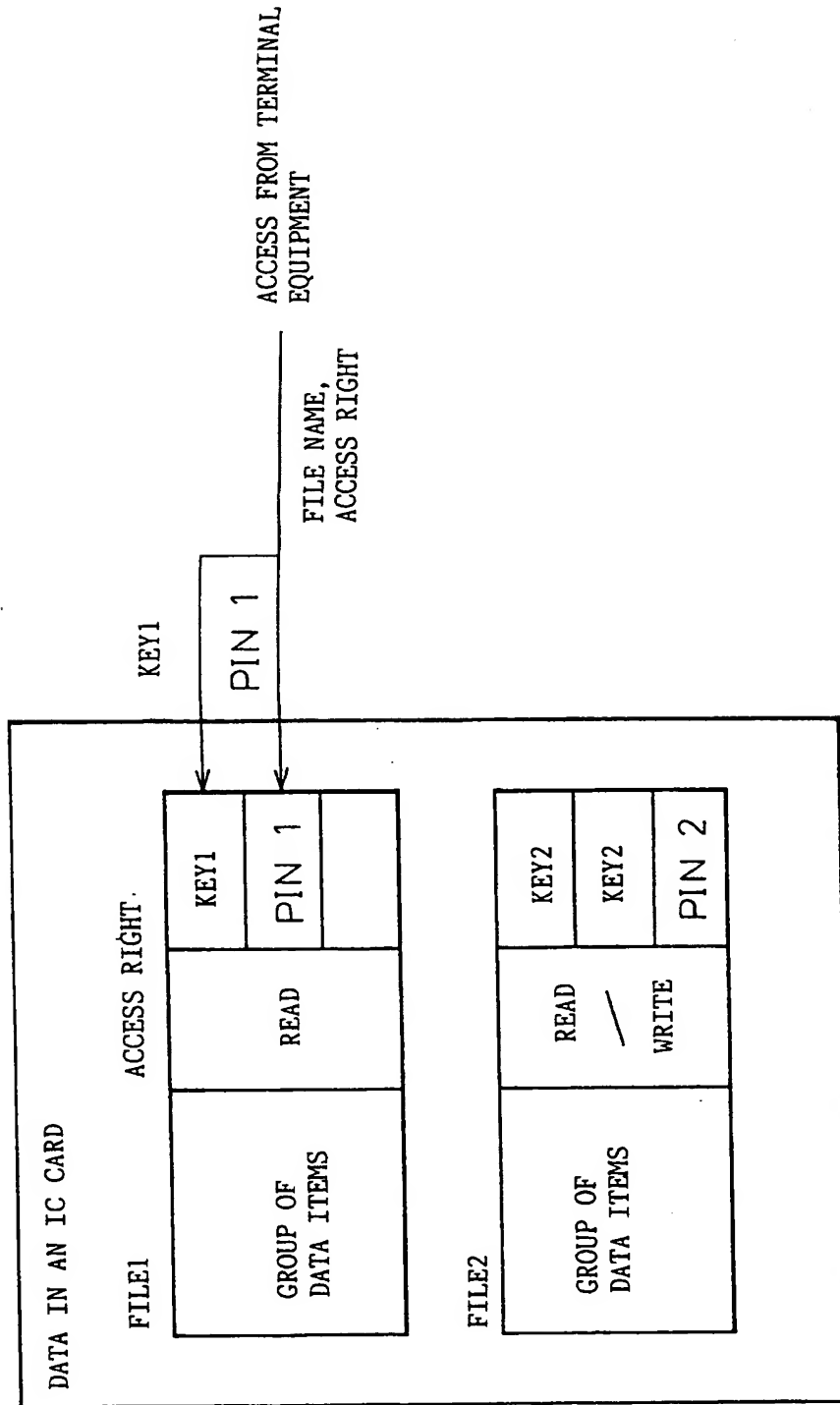


Fig.2

| ITEM NO. | NAME OF DATA ITEM | DATA ITEM VALUE |
|---------------------|----------------------|-----------------------------------|
| 1 | NAME | FUJI TARO |
| 2 | HOME ADDRESS | YOKOHAMA-SHI, KOHOKU-KU, ... |
| 3 | HOME PHONE NO. | 045-234-5678 |
| 4 | OFFICE | ox CO. LTD. |
| 5 | OFFICE ADDRESS | KAWASAKI-SHI, NAKAHARA-KU, ... |
| 6 | OFFICE PHONE NO. | 044-222-1111 |
| 7 | DATE OF BIRTH | AUG. 1, 1960 |
| 8 | BLOOD TYPE | AB |
| | | |
| N | XXX | OOOO |

Fig.3

| ITEM NO. | NAME OF DATA ITEM | ACCESS CHECK DATA | | | | DATA ITEM VALUE |
|----------------|-------------------|---|---|---|----------------|-----------------------------------|
| 1 | NAME | AC CODE ₁₁ ACCESS RIGHT ₁₁ | AC CODE ₁₂ ACCESS RIGHT ₁₂ | AC CODE ₁₃ ACCESS RIGHT ₁₃ | ---- | FUJI TARO |
| 2 | HOME ADDRESS | AC CODE ₂₁ ACCESS RIGHT ₂₁ | AC CODE ₂₂ ACCESS RIGHT ₂₂ | AC CODE ₂₃ ACCESS RIGHT ₂₃ | ---- | YOKOHAMA-SHI, KOHOKU-KU, ... |
| 3 | HOME PHONE NO. | AC CODE ₃₁ ACCESS RIGHT ₃₁ | AC CODE ₃₂ ACCESS RIGHT ₃₂ | AC CODE ₃₃ ACCESS RIGHT ₃₃ | ---- | 045-234-5678 |
| 4 | OFFICE | AC CODE ₄₁ ACCESS RIGHT ₄₁ | AC CODE ₄₂ ACCESS RIGHT ₄₂ | AC CODE ₄₃ ACCESS RIGHT ₄₃ | ---- | ox CO. LTD. |
| 5 | OFFICE ADDRESS | AC CODE ₅₁ ACCESS RIGHT ₅₁ | AC CODE ₅₂ ACCESS RIGHT ₅₂ | AC CODE ₅₃ ACCESS RIGHT ₅₃ | ---- | KAWASAKI-SHI, NAKAHARA-KU, ... |
| 6 | OFFICE PHONE NO. | AC CODE ₆₁ ACCESS RIGHT ₆₁ | AC CODE ₆₂ ACCESS RIGHT ₆₂ | AC CODE ₆₃ ACCESS RIGHT ₆₃ | ---- | 044-222-1111 |
| 7 | DATE OF BIRTH | AC CODE ₇₁ ACCESS RIGHT ₇₁ | AC CODE ₇₂ ACCESS RIGHT ₇₂ | AC CODE ₇₃ ACCESS RIGHT ₇₃ | ---- | AUG. 1, 1960 |
| 8 | BLOOD TYPE | AC CODE ₈₁ ACCESS RIGHT ₈₁ | AC CODE ₈₂ ACCESS RIGHT ₈₂ | AC CODE ₈₃ ACCESS RIGHT ₈₃ | ---- | AB |
| | | | | | | |
| N | DATA _N | AC CODE _{N1} ACCESS RIGHT _{N1} | AC CODE _{N2} ACCESS RIGHT _{N2} | AC CODE _{N3} ACCESS RIGHT _{N3} | ---- | △△△ |

Fig. 4

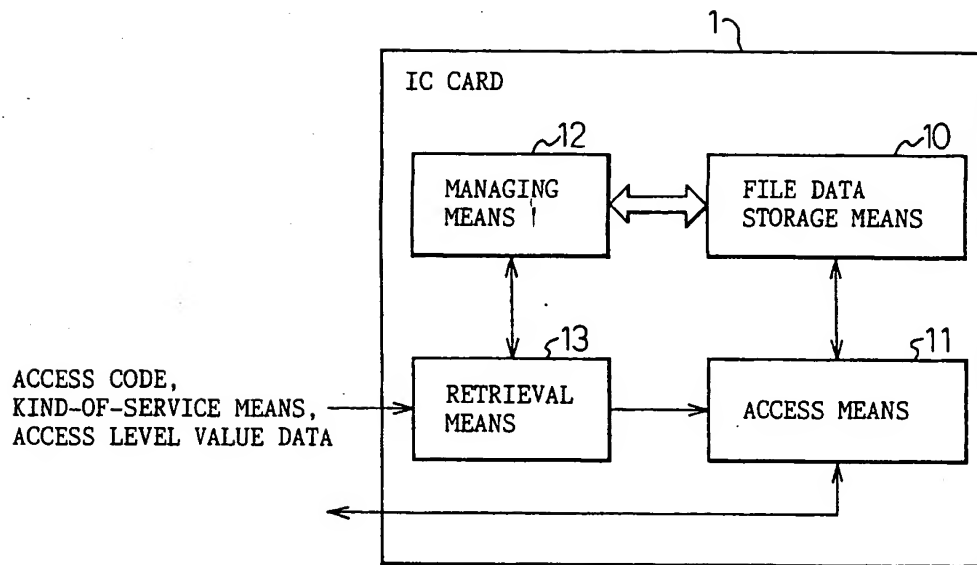


Fig.5

| GROUP OF DATA ITEMS | | | | | | DI ₁ | | DATA ITEM VALUE | |
|---------------------|-------------------|-------------------|--------------|-----------|--------------|------------------|--------------|-----------------|-----------------------------------|
| KEY | | | | | | KY ₁ | | | |
| PIN | | | | | | PIN ₁ | | | |
| ITEM NO. | NAME OF DATA ITEM | ACCESS CHECK DATA | | | | | | | |
| | | SERVICE A | | SERVICE B | | SERVICE C | | | |
| | | LEVEL | ACCESS RIGHT | LEVEL | ACCESS RIGHT | LEVEL | ACCESS RIGHT | | |
| 1 | NAME | | | | | | | ----- | FUJI TARO |
| 2 | HOME ADDRESS | | | | | | | ----- | YOKOHAMA-SHI, KOHOKU-KU, ... |
| 3 | HOME PHONE NO. | | | | | | | ----- | 045-234-5678 |
| 4 | OFFICE | | | | | | | ----- | ox CO., LTD. |
| 5 | OFFICE ADDRESS | | | | | | | ----- | KAWASAKI-SHI, NAKAHARA-KU, ... |
| 6 | OFFICE PHONE NO. | | | | | | | ----- | 044-222-1111 |
| 7 | DATE OF BIRTH | | | | | | | ----- | AUG. 1, 1960 |
| 8 | BLOOD TYPE | | | | | | | ----- | AB |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Fig.6

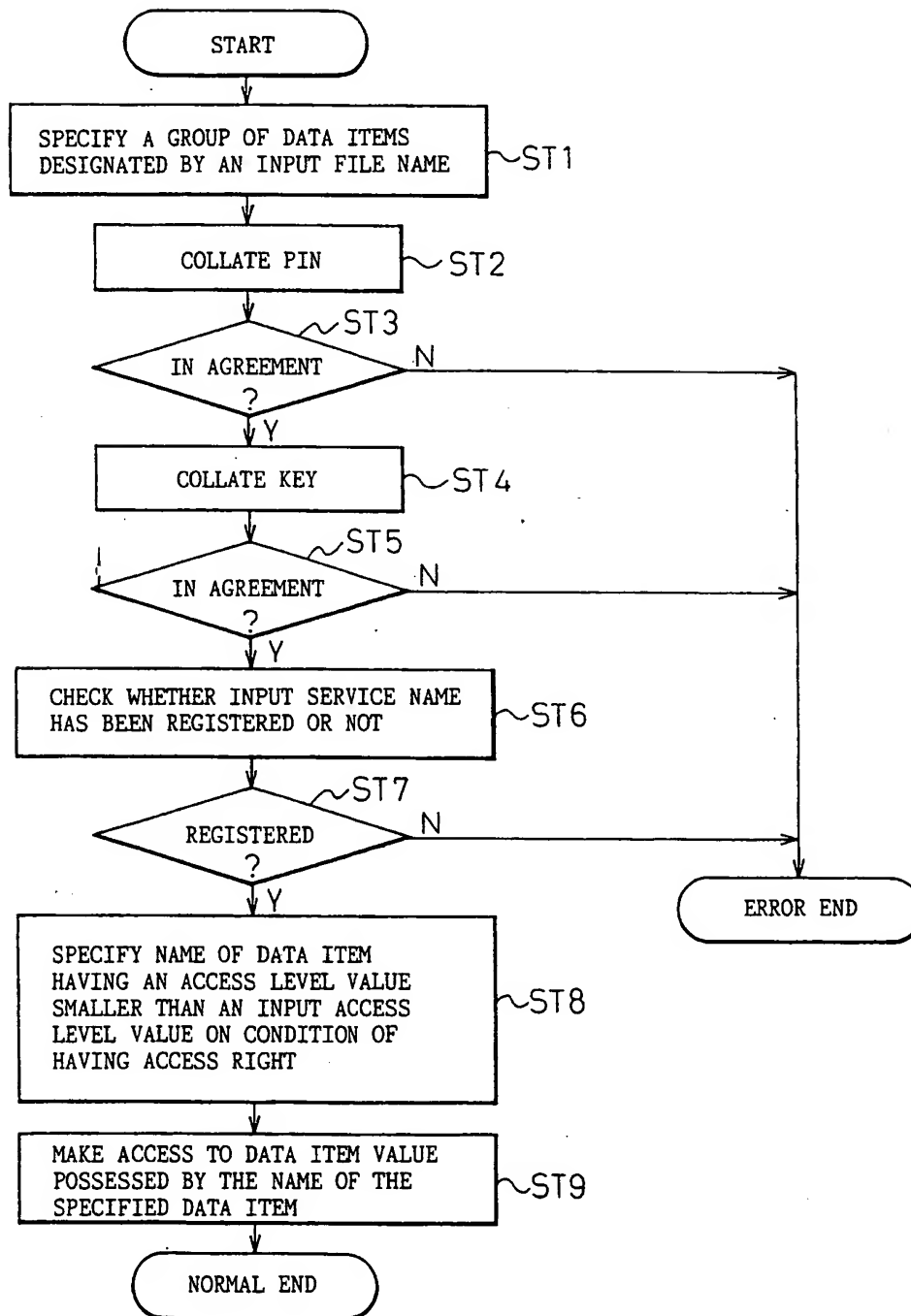


Fig.7

| |
|-----------------------------------|
| FUJI TARO |
| (NULL DATA) |
| (NULL DATA) |
| ox CO., LTD. |
| KAWASAKI-SHI, NAKAHARA-KU, ... |
| 044-222-1111 |
| (NULL DATA) |
| (NULL DATA) |

Fig. 8

| SPECIFIC ACCESS LEVEL VALUE | SERVICE A | SERVICE B | SERVICE C | --- | NAME OF DATA ITEM | DATA ITEM VALUE |
|-----------------------------------|-----------|-----------|-----------|-----|----------------------|----------------------------|
| 10 | ED | ED | — | --- | NAME | FUJI TARO |
| 11 | — | | | --- | NAME | FUJI |
| 20 | 10 | 10 | ED | --- | HOME ADDRESS | YOKOHAMA-SHI, KOHOKU-KU |
| 30 | 20 | 20 | 20 | --- | HOME PHONE NO. | 045-234-5678 |
| --- | --- | --- | --- | --- | | |
| 60 | 50 | — | 50 | | DATE OF BIRTH | MAR. 8, 1967 |
| 70 | 60 | 40 | — | | BLOOD TYPE | A |
| --- | --- | --- | --- | --- | | |
| NN | | | | | | |
| 99 | 90 | 90 | 90 | | | |

SPECIFIC
ACCESS
LEVEL
VALUE

ADDRESS
CORRES. TO
SERVICE A

SPECIFIC
ACCESS
LEVEL
VALUE

ADDRESS
CORRES. TO
SERVICE B

SPECIFIC
ACCESS
LEVEL
VALUE

ADDRESS OF AN ITEM OF
THE CLOSEST ACCESS
LEVEL VALUE

Fig.9

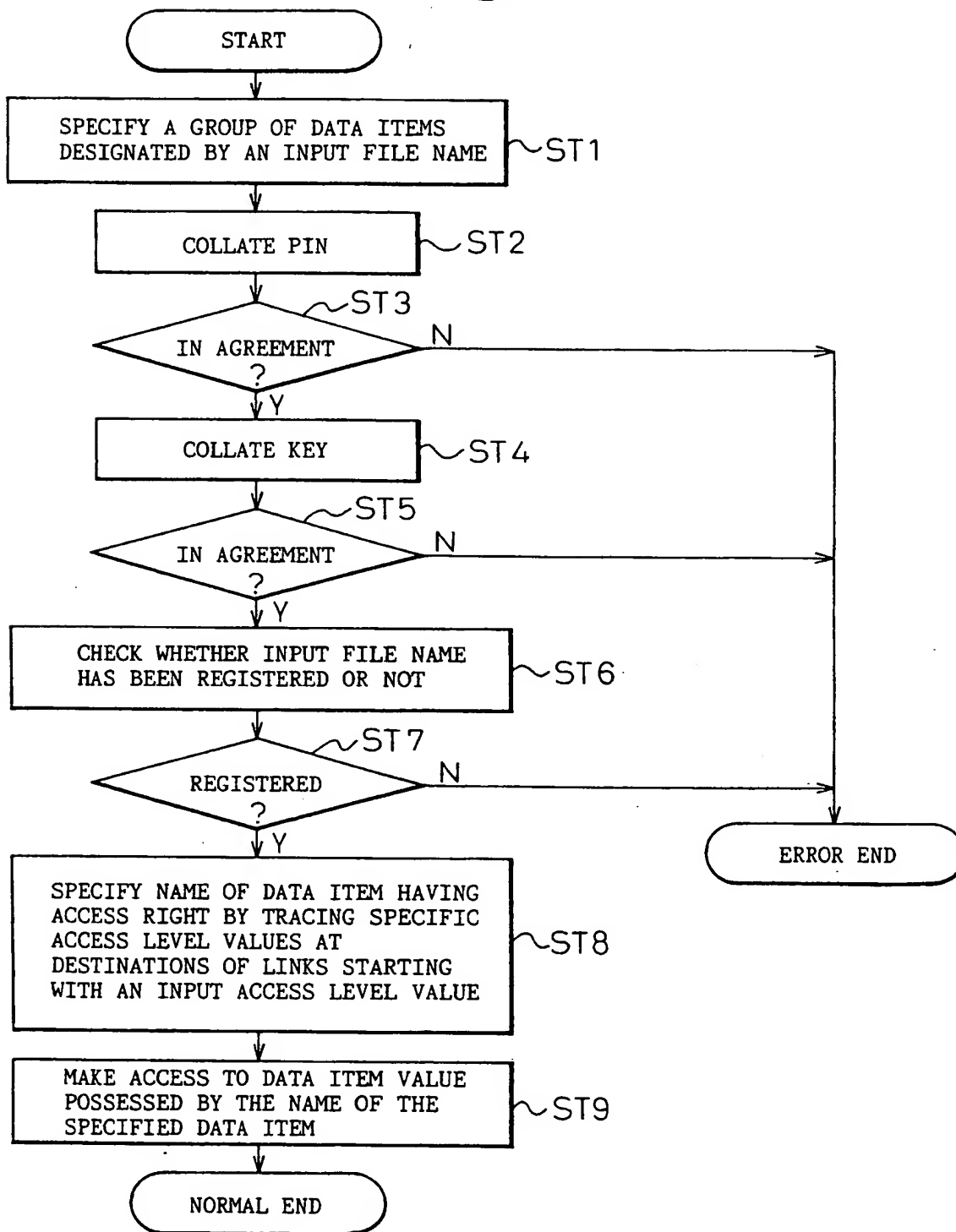


Fig.10

| | |
|------------------|-----------------------------------|
| NAME | FUJI TARO |
| OFFICE | ox CO., LTD. |
| OFFICE ADDRESS | KAWASAKI-SHI, NAKAHARA-KU, ... |
| OFFICE PHONE NO. | 044-222-1111 |

Fig.11

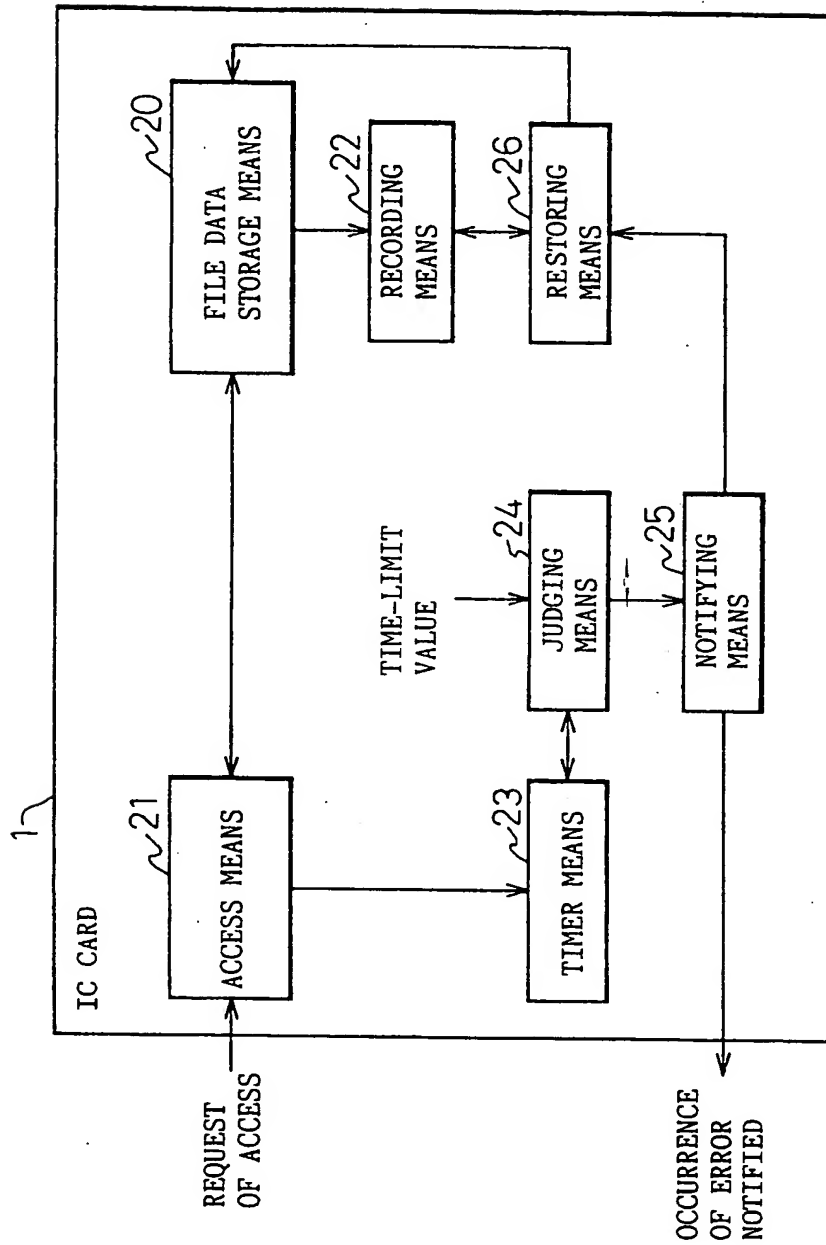


Fig.12

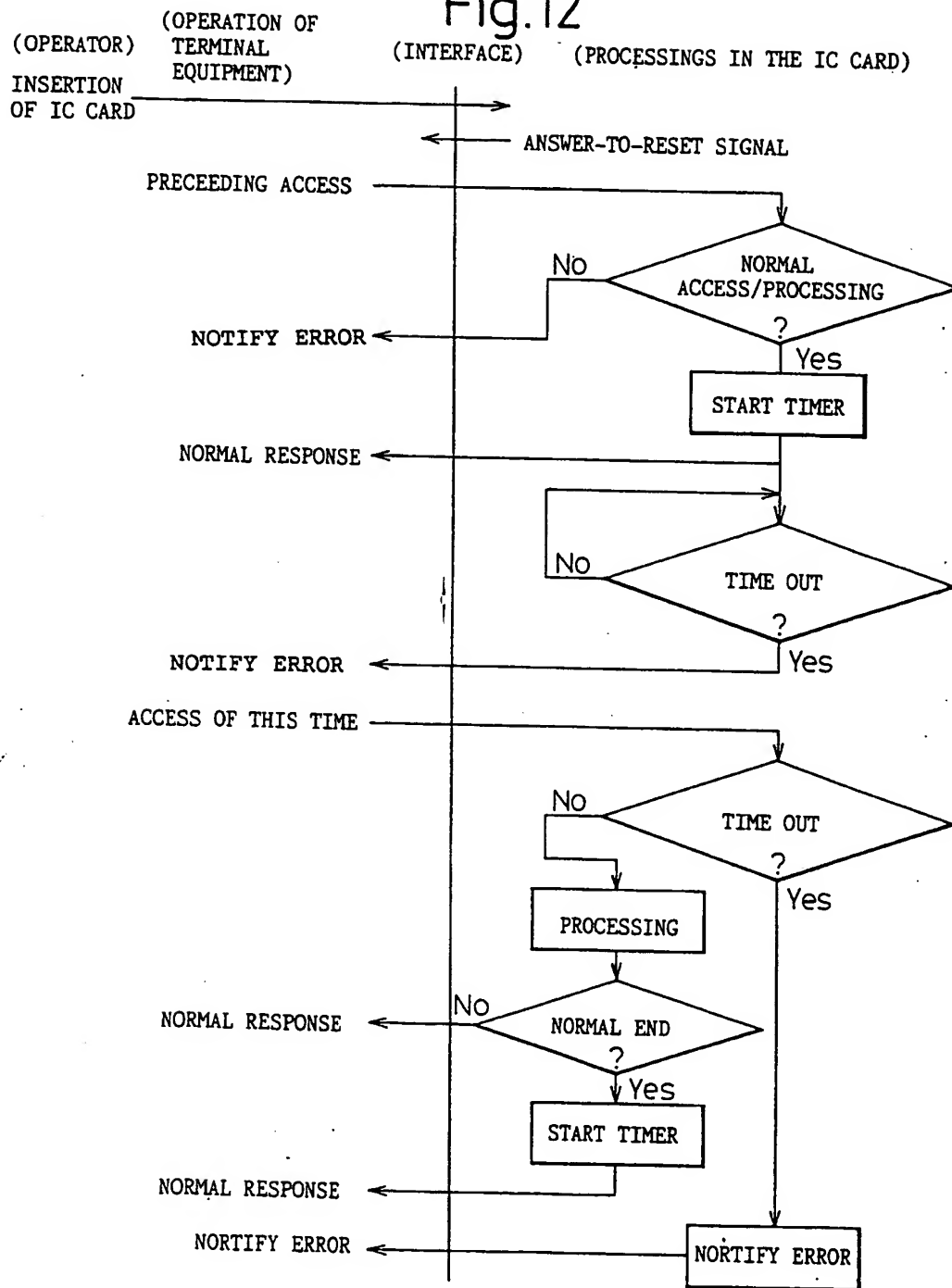


Fig.13

(OPERATION OF
TERMINAL
EQUIPMENT)

(INTERFACE)

(PROCESSINGS IN THE IC CARD)

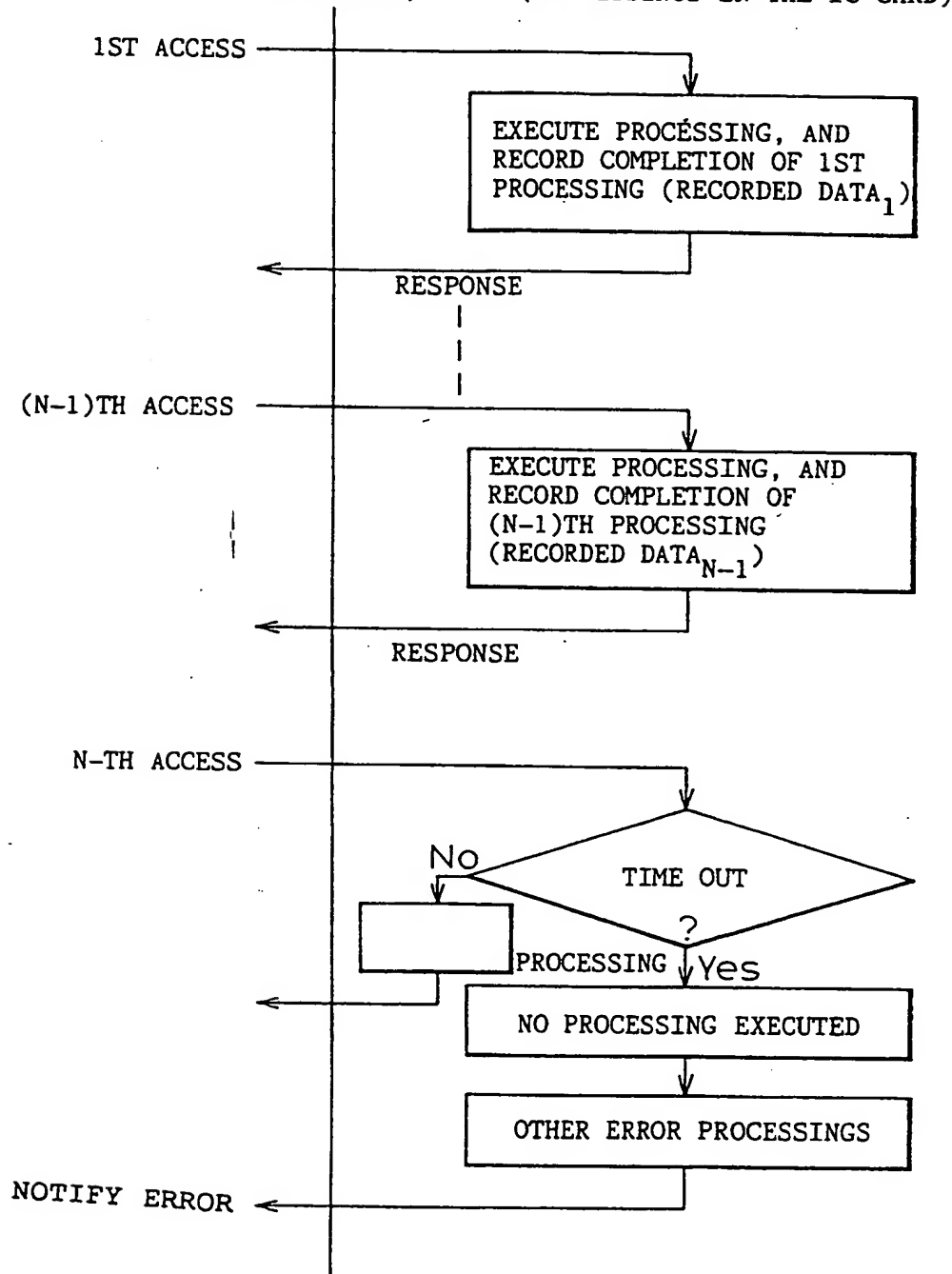
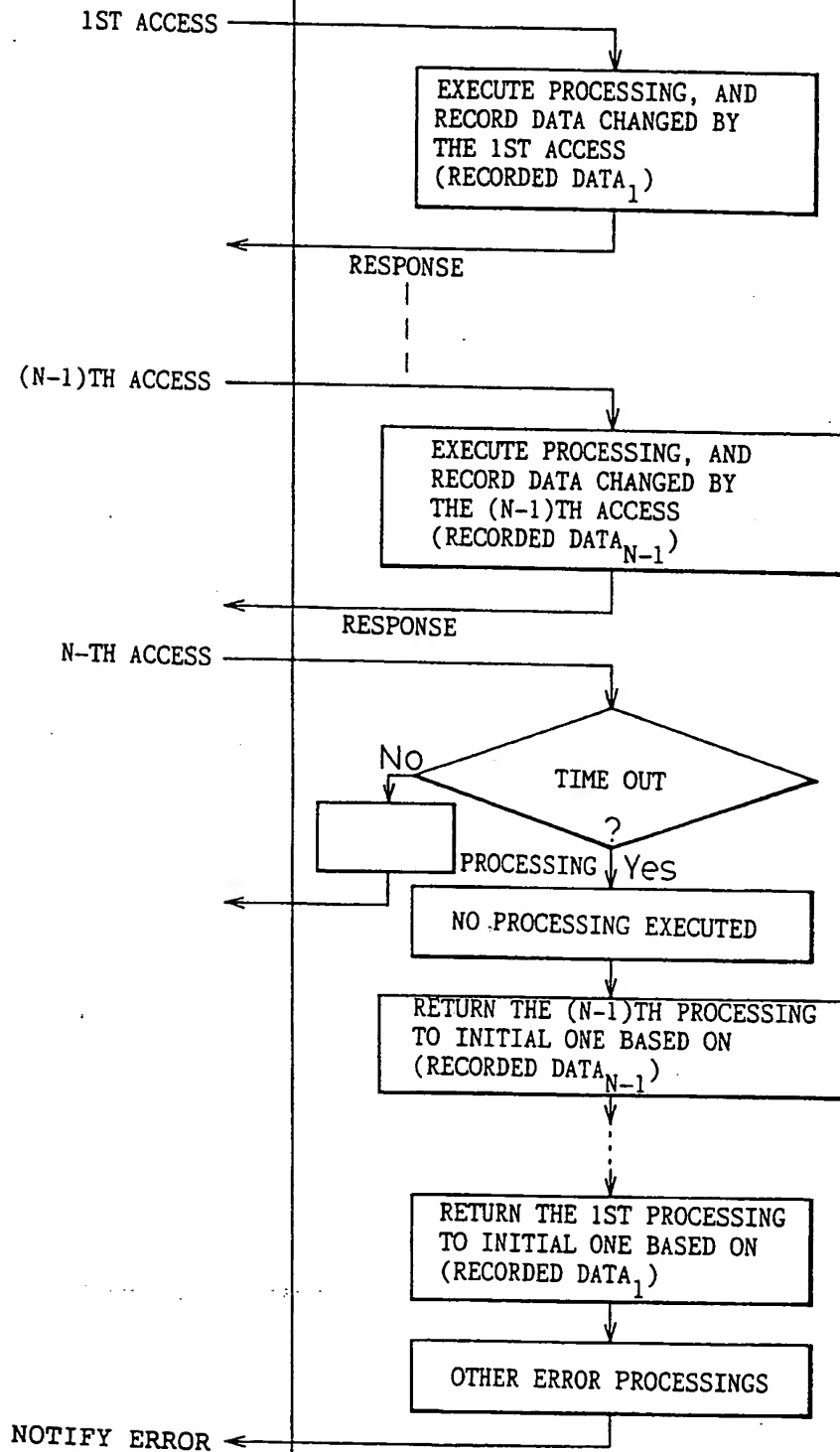


Fig.14

(OPERATION OF
TERMINAL
EQUIPMENT)

(INTERFACE)

(PROCESSINGS IN THE IC CARD)



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP93/01595

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl⁵ G06K19/00, 17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl⁵ G06K19/00, 17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926 - 1993

Kokai Jitsuyo Shinan Koho 1971 - 1993

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---|-----------------------|
| X | JP, A, 62-257555 (Toppan Moore Co., Ltd.), November 10, 1987 (10. 11. 87), (Family: none) | 1-6 |
| X | JP, A, 62-177696 (Hitachi, Ltd.), August 4, 1987 (04. 08. 87), (Family: none) | 1-6 |
| X | JP, A, 2-53154 (Toshiba Corp.), February 22, 1990 (22. 02. 90), (Family: none) | 1-6 |
| X | JP, A, 1-295385 (NEC Corp.), November 29, 1989 (29. 11. 89), (Family: none) | 1-6 |
| Y | JP, A, 61-160174 (Nippon Telegraph & Telephone Corp.), July 19, 1986 (19. 07. 86), (Family: none) | 7 |
| Y | JP, U, 61-176667 (Omron Corp.), November 4, 1986 (04. 11. 86), (Family: none) | 7, 10 |
| Y | JP, A, 60-181891 (Omron Corp.), September 17, 1985 (17. 09. 85), (Family: none) | 8 |

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

January 24, 1994 (24. 01. 94)

Date of mailing of the international search report

February 15, 1994 (15. 02. 94)

Name and mailing address of the ISA/

Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP93/01595

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| Y | JP, A, 61-296486 (Fujitsu Ltd.), December 27, 1986 (27. 12. 86), (Family: none) | 8 |
| Y | JP, A, 4-137081 (Fuji Photo Film Co., Ltd.), May 12, 1992 (12. 05. 92), (Family: none) | 10, 11 |